UNITED STATES DISTRICT COURT FOR THE

DISTRICT OF MARYLAND

SOUTHERN DIVISION

HOPE TURNER
2551 Magnolia Fair Way
Spring, Texas 77386

individually and on behalf of all others similarly situated,

Plaintiff,

vs.

MARRIOTT INTERNATIONAL, INC.,
(resident of Montgomery County, Maryland)
10400 Fernwood Road
Bethesda, Maryland 20817

Serve On:

The Corporation Trust Inc.
2405 York Road
Suite 201
Lutherville Timonium, MD 21093-2264

and

STARWOOD HOTELS AND RESORTS WORLDWIDE, LLC (resident of Montgomery County, Maryland)
10400 Fernwood Road
Bethesda, Maryland 20817

Serve On:

The Corporation Trust Inc.
2405 York Road
Suite 201
Lutherville Timonium, MD 21093-2264

Defendants.

Case No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Hope Turner, on behalf of herself and all others similarly situated, alleges the following against Marriott International, Inc., Starwood Hotels and Resorts Worldwide, LLC, and those acting on their behalves (collectively, Defendants). Plaintiff's allegations are based upon her personal knowledge of the facts pertaining to herself, and for all other matters, on information and belief, the investigations of counsel, and review of public documents.

Introduction

1. On November 30, 2018, Marriott, parent company of Starwood, announced a massive data breach compromising the personal information of a half billion people whose information Defendants stored in the Starwood guest reservation database.

2. The information taken includes names, phone numbers, mailing and email addresses, passport numbers, Starwood Preferred Guest account data, dates of birth, gender, arrival and departure information, reservation dates, and communication preferences. For some, the information taken also includes payment card numbers and expiration dates.

3. That Defendants failed to detect or prevent this data breach is particularly astonishing. According to Marriott, the hackers first accessed Starwood's systems in 2014 and Defendants did not detect them until September 2018. During that same period, Starwood failed to prevent numerous breaches, including a payment card data breach at approximately 100 of its properties. Despite these obvious danger signs, Defendants still failed to adequately secure the Starwood reservation system, a massive database that should have been protected by the most sophisticated security controls available.

4. As a result of Defendants' failure to protect the customer information they hoarded, Plaintiff and others already have suffered fraud, identity theft, and financial harm, and many millions more now are subject to a heightened, imminent risk of such harm.

Parties

5. Plaintiff Hope Turner is a resident and citizen of Texas. Ms. Turner provided Defendants with her personal information, which was compromised in the data breach.

6. Defendant Marriott International, Inc. is a Delaware corporation with its principal office at 10400 Fernwood Rd., Bethedsa, Maryland, 20817 (Montgomery County). Marriott is the parent company of Starwood.

7. Defendant Starwood Hotels & Resorts Worldwide, LLC is a Delaware corporation with its principal office at 10400 Fernwood Rd., Bethedsa, Maryland, 20817 (Montgomery County). Starwood is an indirect, wholly-owned subsidiary of Defendant Marriott.

Jurisdiction and Venue

8. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because at least one Class member is of diverse citizenship from at least one Defendant, there are 100 or more Class members, and the aggregate amount in controversy is greater than $5 million, exclusive of attorneys' fees, interest, and costs.

9. This Court has personal jurisdiction over Marriott and Starwood because both companies are organized under the laws of Maryland, maintain their principal offices in Maryland, regularly conduct business in this state, and the claims for relief relate to acts and omissions occurring within this forum.

10. Venue is proper in this District pursuant to 28 U.S.C. § 1931(b)(3) because this Court has personal jurisdiction over Defendants, a substantial portion of the alleged wrongdoing occurred in this District, and both Defendants have sufficient contacts within this District.

Venue also is proper pursuant to 28 U.S.C. § 1931(b)(2) because a substantial part of the events or omissions giving rise to the claims arose in this District.

Factual Allegations

Marriott Announced that Starwood's Systems Were Breached for Four Years

11. Marriott is a global hotel conglomerate. According to its 2017 Annual Report, Marriott owns 1,959 properties and operates another 4,432 franchised and licensed properties, for a combined total of over 1,200,000 rooms in its portfolio. Marriott hotels include well-known brands such as Marriott, Ritz-Carlton, Courtyard, and Residence Inn.

12. Starwood Hotels & Resorts Worldwide competed with Marriott, until Marriott acquired Starwood in September 2016 for $13.6 billion. At the time of the Marriott acquisition, Starwood oversaw over 1,000 properties. Starwood properties included W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Meridien Hotels & Resorts, Four Points by Sheraton, and Design Hotels.

13. On November 30, 2018, Marriott confirmed that there had been unauthorized access to the Starwood guest reservation database, "which contained guest information relating to reservations at Starwood properties on or before September 10, 2018." This massive database "contains information on up to approximately 500 million guests who made a reservation at a Starwood property."

14. Marriott claims that it first noticed the unauthorized activity on September 8, 2018, when it received an alert from an internal tool that a third-party had attempted to access the Starwood guest reservation database.

15. After engaging "leading security experts to help determine what occurred," Marriott learned that there had been unauthorized access to the Starwood network since 2014. In other words, neither Starwood nor Marriott detected the intrusion for years after it began.

16. The investigation also revealed that an unauthorized party had copied and encrypted then-unidentified information and "took steps toward removing it." On November 10, 2018, Marriott decrypted the information and discovered it came from the Starwood guest reservation database.

17. It is almost certain that the hackers exfiltrated massive amounts of personal information during their four years of access. Marriott's description of the breach is consistent with the final stages of the standard "attack lifecycle" in a successful data breach. Hackers typically download sensitive information from an inadequately secured database, stage the files on a server that has inadequately controlled internet access, encrypt the data using the company's own processing power, and then exfiltrate the data. If the hackers are able to encrypt the data without being detected, downloading it is trivial and would have occurred almost immediately.

18. According to Marriott, those who made reservations on or before September 10, 2018 at a Starwood property were implicated. Affected Starwood properties include W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Meridien Hotels & Resorts, Four Points by Sheraton, and Design Hotels that participate in the Starwood Preferred Guest ("SPG") program. Starwood-branded timeshare properties were also included in the breach.

19. Marriott is providing free enrollment in WebWatcher for one year. As of November 30, 2018, WebWatcher enrollment is limited to the United States, Canada, and the United Kingdom. WebWatcher enrollees in the United States will also be offered fraud

consultation services from Kroll and reimbursement coverage. This leaves individuals outside of the United States, Canada, and the United Kingdom with no monitoring tools, and individuals outside of the United States with no fraud consultation services or reimbursement coverage, unless they enroll in comparable services themselves.

Defendants Knew They Were At Risk Of A Cyberattack

20. When individuals make hotel reservations, hotels ask for their personal information, including credit card information, names, birthdates, mailing addresses, email addresses, passport numbers, and arrival and departure information. Hotels possess significant personal information about individuals who have stayed in their rooms.

21. Cyberattacks against hotel groups have been on the rise because this information is valuable. Major hotel groups that have permitted data breaches in recent years include InterContinental Hotels Group, Hyatt Hotels (at least twice), the Trump Hotel Collection (at least three times), Kimpton Hotels, and Mandarin Oriental hotels, among others.

22. In fact, Starwood and Marriott experienced several prior breaches, but still failed to shore up their deficient information security controls. First, in November 2015, Starwood announced it had suffered a data breach that was eventually discovered to have compromised payment cards used at restaurants, gift shops, and other point of sale systems at more than 100 of its properties. In a January 22, 2016 letter addressing the incident, Starwood's then-President Sergio Rivera promised that "protecting the security of our customers' personal information is a top priority for Starwood" and there was "no indication that our guest reservation system or Starwood Preferred Guest membership systems were impacted."

23. According to Forbes, Marriott and Starwood also experienced breaches that they did not publicly announce. "Prior to the four-year-old breach being discovered, Marriott

suffered at least one previously unreported hack, including an infection that hit the company's own cyber-incident response team, *Forbes* has learned. And there's evidence Russian cybercriminals have breached Starwood Web servers."

24. Many of these earlier hotel breaches impacted only point-of-sale systems on the periphery of the hotel networks, and primarily targeted credit card information from gift shops and restaurants. Marriott and Starwood, however, knew that if data collected from the hotel's periphery was appealing to cybercriminals, the reservation system data was even more valuable and lucrative to hackers, and its compromise would be more damaging to customers. In fact, in a January 22, 2016 letter addressing that breach, Starwood promised that "protecting the security of our customers' personal information is a top priority for Starwood" and there was "no indication that our guest reservation system or Starwood Preferred Guest membership systems were impacted."

25. Despite this notice, neither Marriott nor Starwood shored up their demonstrably deficient information systems.

Starwood Promised That Personal Information Would Be Protected

26. Starwood's representations also indicated that it would take steps to protect the personal information acquired. Its privacy policy effective as of January 22, 2012, which was still on its website as of October 2017 stated as follows:

> Starwood recognizes the importance of information security, and is constantly reviewing and enhancing our technical, physical, and logical security rules and procedures. All Starwood owned web sites and servers have security measures in place to help protect your PII against accidental, loss, misuse, unlawful or unauthorized access, disclosure, or alteration while under our control. Although "guaranteed security" does not exist either on or off the Internet, we safeguard your information using appropriate administrative, procedural and technical safeguards, including password controls, "firewalls" and the use of up to 256-bit encryption based on a Class 3 Digital Certificate issued by VeriSign, Inc. This allows for the use of Secure Sockets Layer (SSL), an encryption method used to help protect your data from interception and hacking while in transit.

27. Starwood's Online Privacy Statement, revised on October 5, 2017, stated that: "Your personal data will be kept in a form which enables [*sic*] to identify you for no longer than is necessary for the purposes for which we collected and use your data . . . ."

28. Marriott stated that it seeks "to use reasonable organization, technical and administrative measures to protect Personal Information."

The Cybersecurity Protecting Starwood's Reservation System Was Insufficient

29. While Marriott's public statements attempt to put the best spin possible on the facts of this breach, the limited information Defendants have provided already makes clear that their cybersecurity controls were woefully (and illegally) deficient.

30. That hackers had accessed the Starwood network for four years without being detected, particularly when the earlier breaches prompted security audits, demonstrates that Defendants' systems lacked adequate intrusion detection capabilities.

31. In fact, Defendants should have implemented database monitoring tools to detect suspicious database queries and large data exports like these. These actions should have immediately set off alarms and triggered alerts to security personnel, who should have been monitoring Defendants' systems at all times, day and night. It is clear that these monitoring and alerting systems were not in place or were ignored.

32. Marriott also explains that Starwood encrypted customers' payment card information, but the encryption keys used to decrypt that information also "may" have been taken. Obviously, failing to secure important encryption keys is negligent by any measure. But Defendants' uncertainty about the theft of the keys demonstrates more fundamental information security flaws. If Defendants had implemented reasonable and appropriate information security

controls, they would know – one way or the other – whether the encryption keys are secure. Instead, Defendants either chose not to monitor their systems or failed to stop these hackers from deleting or modifying the computer files that should record their activities, a common hacker technique.

The Marriott Data Breach Harmed Individuals, and Additional Fraud Will Result

33. Consumers who have been victims of data breaches are much more likely to become victims of identity fraud than those who have not. Further, each additional data breach an individual is involved in increases his or her risk of identity fraud.

34. The Federal Trade Commission defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(9). "Identifying information," in turn, "means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including names, dates of birth, and passport numbers. 17 C.F.R. § 248.201(8).

35. As the FTC explains, "[o]nce identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."

36. The Bureau of Justice Statistics has reported that, even if data thieves have not caused financial harm, data breach victims "reported spending an average of about 7 hours clearing up the issues."

37. Identity thieves often hold onto personal information obtained to commit fraud years after free credit monitoring programs expire. Even so-called State-sponsored hacking groups, after providing the stolen information to their government client, quickly repackage and sell the same stolen information to identity thieves.

38. In fact, the harms here are likely to be more severe because Defendants announced the breach well after it occurred. According to a 2017 study by performed New Javelin Strategy, "The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."

Plaintiff's Experience

39. Ms. Turner has stayed at multiple Starwood properties throughout the Class Period. She booked her stays by using her credit cards and providing Defendants with her personal information, as required by Defendants. Ms. Turner's personal information was compromised in the data breach and she has suffered identity theft as a result. For example, unknown persons attempted to obtain approximately $700 from one of Ms. Turner's existing accounts. After Defendants discovered the data breach, but before they publicly announced it, Ms. Turner detected a $5,500 charge on her account that she had not authorized. After investigating, Ms. Turner discovered that the money had been wired to a third party using her personal information. Ms. Turner has spent time and resources resolving this issue, freezing her credit with all three credit bureaus, and signing up for credit monitoring, including with Equifax and LifeLock. Had Ms. Turner known that Defendants were inadequately protecting her personal information, she would not have stayed at Starwood properties.

Class Allegations

40. Under Federal Rule of Civil Procedure 23(b)(2) and (b)(3), Plaintiff asserts claims on behalf of the following Class:

> **Class:** All persons in the United States whose personal information was compromised in the data breach announced by Marriott on November 30, 2018.

Texas Subclass: All persons in Texas whose personal information was compromised in the data breach announced by Marriott on November 30, 2018.

Excluded from the Class are Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class are any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

41. **Numerosity: Federal Rule of Civil Procedure 23(a)(1).** The Class members are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. Plaintiff is informed and believes—based on Marriott's statements to the press—that there are approximately 500,000,000 class members. Those individuals' names and addresses are available from Defendants' records.

42. **Commonality and Predominance: Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** The action involves common questions of law and fact, which predominate over any questions affecting individual class members, including:

a. Whether Defendants knew or should have known that their reservation systems were vulnerable to unauthorized access

b. Whether Defendants failed to take adequate and reasonable measures to ensure their data systems were protected

c. Whether Defendants failed to take available steps to prevent and stop the breach from happening; or

d. Whether Defendants breached any duty to protect the Personal Information of Plaintiff and Class members by failing to provide adequate data security;

43. **Typicality: Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of other Class members' claims because Plaintiff and Class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

44. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate class representative because her interests do not conflict with the interests of Class members who she seeks to represent, Plaintiff has retained counsel competent and experienced in complex class action litigation and data breach litigation, and Plaintiff intends to prosecute this action vigorously. The Class members' interests will be fairly and adequately protected by Plaintiff and her counsel.

45. **Declaratory and Injunctive Relief: Federal Rule of Civil Procedure 23(b)(2).** The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Defendants. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class members and impair their interests. Defendants have acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

46. **Superiority: Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudicating of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek

redress for Defendants' wrongful conduct. Even if Class members could afford litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

First Cause of Action

Negligence (on behalf of Plaintiff and the Class)

47. Plaintiff realleges the preceding and subsequent paragraphs as though fully set forth herein.

48. Defendants owed Plaintiff and Class members a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the personal information in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. This duty included, among other things:

a. Designing, maintaining, and testing Defendants' security systems to ensure that Plaintiff's and Class members' personal information was adequately secured and protected;

b. Implementing processes that would detect a breach of their security systems in a timely manner;

c. Maintaining data security measures consistent with industry standards and their own representations;

d. Properly investigating the security of Starwood's systems after Starwood detected the 2016 Starwood breach and assured customers that the reservation system was not compromised.

49. Defendants' duties to use reasonable care arose from several sources, including a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices.

50. Defendants' duties also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such as Defendants. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

51. Defendants' duties also arose under the Maryland Personal Information Protection Act. That statute mandated that businesses that own personal information of an individual residing in Maryland "shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned . . . and the nature and size of the business and its operations." Maryland Code Ann., Comm. Law Art. ("CL") § 14-3503(a).

52. Defendants breached the duties it owed to Plaintiff and Class members described above and was thus negligent. Defendants breached these duties by, among other things failing to:

a. Design, maintain, and test Defendants' security systems to ensure that Plaintiff's and Class members' personal information was adequately secured and protected;

b. Implement processes that would detect a breach of their security systems in a timely manner;

c. Maintain data security measures consistent with industry standards and their own representations; and

d. Investigate reasonably the scope of the 2016 Starwood breach.

53. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class members, their personal information would not have been compromised.

54. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

Second Cause of Action

Negligence Per Se (on behalf of Plaintiff and the Class)

55. Plaintiff realleges the preceding and subsequent paragraphs as though fully set forth herein.

56. Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such as Defendants. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

57. The Maryland Personal Information Protection Act also mandates that businesses that own personal information of an individual residing in Maryland "shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the

personal information owned . . . and the nature and size of the business and its operations." CL § 14-3503(a).

58. Defendants violated both of these statutes by failing to use reasonable measures to protect personal information and not complying with industry standards. Defendants' conduct was particularly unreasonable given the vast amount of personal information they obtained and stored, the years-long period of exposure, and their prior breaches that overlapped in time with this one.

59. Defendants' violation of Section 5 of the FTC Act (and similar state statutes), as well as their violation of the Maryland Personal Information Protection Act, constitutes negligence *per se*.

60. Plaintiff and Class members are within the class of persons Section 5 of the FTC Act (and similar state statutes) and the Maryland Personal Information Protection Act were intended to protect.

61. The harm that occurred is the type of harm the FTC Act (and similar state statutes) and the Maryland Personal Information Act were intended to guard against.

62. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

Third Cause of Action

Unjust Enrichment (on behalf of Plaintiff and the Class)

63. Plaintiff realleges the preceding and subsequent paragraphs as though fully set forth herein.

64. Plaintiff and Class members conferred a monetary benefit on Defendants in the form of moneys paid for reservations and stays at Starwood hotels.

65. Defendants appreciated or had knowledge of the benefits conferred on them by Plaintiff and Class members.

66. The monies paid to stay at Starwood hotels that Plaintiff and Class members paid (directly or indirectly) to Defendants were supposed to be used by Defendants, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

67. As a result of Defendants' conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between hotel stays with the reasonable data privacy and security practices that Plaintiff and Class members paid for, and the inadequate stays without reasonable data privacy and security practices and procedures that they received.

68. Under principals of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class members because Defendants failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class members paid for and that were otherwise mandated by the FTC Act (and similar state statutes) and the Maryland Personal Information Act.

69. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class members all unlawful or inequitable proceeds received by them.

Fourth Cause of Action

Violation of Maryland's Consumer Protection Act Maryland Code Ann., Comm. Law Article § 13-101, *et seq.* (on behalf of Plaintiff and the Class)

70. Plaintiff realleges the preceding and subsequent paragraphs as though fully set forth herein.

71. Defendants are persons as defined by CL § 13-101(h).

72. Defendants' conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by CL § 13-101(i) and § 13-303.

73. Plaintiff and Class members are "consumers" as defined by CL § 13-101(c).

74. Defendants advertise, offer, or sell "consumer goods" or "consumer services" as defined by CL § 13-101(d).

75. Defendants advertised, offered, or sold goods or services in Maryland and engaged in trade or commerce directly or indirectly affecting the people of Maryland.

76. Defendants engaged in unfair and deceptive trade practices, in violation of CL § 13-301, including:

a. Failing to state a material fact where the failure deceives or tends to deceive; and

b. Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale, lease, or rental.

77. Defendants engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services or with respect to the extension of consumer credit, in violation of CL § 13-303, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class members' personal information, which was a direct and proximate cause of the data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' personal information, including duties imposed by the FTC Act (and similar state statutes) and the Maryland Personal Information Protection Act, which was a direct and proximate cause of the data breach;

d. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Class members' personal information;

e. Omitting, suppressing, and concealing the material fact that they did not conduct a reasonable investigation of the scope of the 2016 Starwood Breach; and

f. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' personal information, including duties imposed by the FTC Act and the Maryland Personal Information Protection Act.

78. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' personal information. Defendants' representations and omissions would have been important to a significant number of consumers in making financial decisions.

79. Defendants intended to mislead Plaintiff and Class members and induce them to rely on their misrepresentations and omissions.

80. Defendants acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded Plaintiff's and Class members' rights. The 2016 Starwood Breach, and those of other hotel companies, put Defendants on notice that their security and privacy protections were inadequate.

81. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft, and a loss of value of their personal information.

82. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

Fifth Cause of Action

Deceptive Trade Practices—Consumer Protection Act Texas Bus. & Com. Code §§ 17.41, *et seq.* (on behalf of Plaintiff and the Texas Subclass)

83. Plaintiff realleges the preceding and subsequent paragraphs above as if fully set forth herein.

84. Defendants are each a "person" as defined by Tex. Bus. & Com. Code § 17.45(3).

85. Plaintiff and the Texas Subclass members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

86. Defendants advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

87. Defendants engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another; and

c. Advertising goods or services with intent not to sell them as advertised.

88. Defendants' false, misleading, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Texas Subclass members' personal information, which was a direct and proximate cause of the data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas' data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the data breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff and Texas Subclass members' personal information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas' data security statute, Tex. Bus. & Com. Code § 521.052;

f. Misrepresenting that they had reasonably investigated the scope of the 2016 Starwood Breach, which was underway at the same time as this breach;

g. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Texas Subclass members' personal information; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and Texas' data security statute, Tex. Bus. & Com. Code § 521.052.

89. Defendants intended to mislead Plaintiff and Texas Subclass members and induce them to rely on its misrepresentations and omissions.

90. Defendants' misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of their data security and ability to protect the confidentiality of consumers' personal information.

91. Defendants had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extent of the personal information in their possession, and generally accepted professional standards in the hotel and cybersecurity industries. Defendants' duty to disclose also arose from their:

a. Possession of exclusive knowledge regarding the security of the data in their systems;

b. Active concealment of the state of their security; and/or

c. Incomplete representations about the security and integrity of their computer and data systems, and their prior data breach, while purposely withholding material facts from Plaintiff and the Texas Subclass that contradicted these representations.

92. Defendants engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Defendants engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

93. Consumers, including Plaintiff and Texas Subclass members, lacked knowledge about deficiencies in Defendants' data security because this information was known exclusively to Defendants. Consumers also lacked the ability, experience, or capacity to secure the personal information in Defendants' possession or to fully protect their interests with regard to their data. Plaintiff and Texas Subclass members lack experience in information security matters and do not have access to Defendants' systems in order to evaluate their security controls. Defendants took advantage of their special skill and access to personal information to hide their inability to protect the security and confidentiality of Plaintiff and Texas Subclass members' personal information.

94. The data breach, which resulted from Defendants' unconscionable business acts and practices, exposed Plaintiff and Texas Subclass members to a wholly unwarranted risk to the safety of their personal information, and caused a substantial hardship to a significant and unprecedented number of consumers. Plaintiff and Texas Subclass members cannot mitigate this unfairness because they cannot undo the data breach.

95. Defendants acted intentionally, knowingly, and maliciously to violate Texas' Deceptive Trade Practices—Consumer Protection Act, and recklessly disregarded Plaintiff and Texas Subclass members' rights. The prior data breach, as well as other recent hotel data breaches, put Defendants on notice that their security and privacy protections were inadequate.

96. As a direct and proximate result of Defendants' unconscionable and deceptive acts or practices, Plaintiff and Texas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their personal information. Defendants' unconscionable and deceptive acts or practices were a proximate cause of Plaintiff's and Texas Subclass members' injuries, ascertainable losses, economic damages, and non-economic damages, including their mental anguish.

97. Defendants' violations present a continuing risk to Plaintiff and Texas Subclass members, as well as to the general public.

98. Plaintiff and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; triable damages for

each act committed intentionally or knowingly; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief which the Court deems proper.

Prayer for Relief

WHEREFORE, Plaintiff, both individually and on behalf of the other Class members, respectfully request this Court enter an order:

a. Certifying the Class and appointing Plaintiff as Class Representative;

b. Declaring that Defendants' conduct was negligent, deceptive, unfair, and unlawful;

c. Enjoining Defendants from engaging in further negligent, deceptive, unfair, and unlawful business practices;

d. Awarding Plaintiff and Class members actual, compensatory, consequential damages, statutory damages, punitive damages, restitution, disgorgement, penalties, and pre- and post-judgment interest, to the extent permitted by the law;

e. Requiring Defendants to take all available measures to mitigate the past and future harms they caused to Plaintiff and other Class members;

f. Awarding Plaintiff and Class members reasonable attorneys' fees and costs; and

g. Granting such other relief as the Court deems just and proper.

Demand for Jury Trial

Plaintiff demands a trial by jury for all issues so triable.

Dated: December 6, 2018

Respectfully Submitted,

/s/ William H. Murphy III

William H. Murphy III (Bar No. 30126)
Jessica H. Meeder (Bar No. 17986)
MURPHY, FALCON & MURPHY, P.A.
One South Street, 23rd Floor
Baltimore, MD 21202
Telephone: (410) 951-8744

Fax: (410) 539-6599
hassan.murphy@murphyfalcon.com
jessica.meeder@murphyfalcon.com

Eric H. Gibbs (*pro hac vice forthcoming)*
David M. Berger (*pro hac vice forthcoming)*
Amanda Karl (*pro hac vice forthcoming)*
GIBBS LAW GROUP LLP
505 14th Street, Suite 1110
Oakland, CA 94612
Tel: (510) 350-9700
Fax: (510) 350-9701
ehg@classlawgroup.com
dmb@classlawgroup.com
amk@classlawgroup.com